数理解析研究所講究録
第 1806 巻 2012 年 134-142

Upper bounds for solutions of exponential Diophantine equations with applications to Fibonacci numbers

Takafumi Miyazaki
(Tokyo Metropolitan University)

2011 年 11 月 1 日

1 Introduction

指数型ディオファントス方程式

$$(*) \qquad a^x + b^y = c^z$$

を考える. ここで, x, y, z は自然数, a, b, c はどの二つも互いに素な固定された 1 より大の自然数とする. ディオファントス近似の理論によって, 方程式 $(*)$ の解の一般的な情報を得ることが出来る. Thue-Siegel の手法の p 進解析法を用いて, Mahler [8] は初めて $(*)$ は高々有限個の解しか持たないことを証明している. 方程式 $(*)$ は, 単数方程式の一つであるとみなせる. 単数方程式の理論によって, 方程式 $(*)$ の解の個数 ($N = N(a, b, c)$ とおく) の上界を得ることが出来る. 特に, [2] の結果を用いれば, 絶対定数の評価:

$$N \leq 2^{36}$$

を得ることが出来る. しかし, 実際は, N は非常に小さいと考えられている. 実際, $N > 3$ となるような三つ組み (a, b, c) を見つけられておらず, そして $N = 3$ となる例はただ一つ知られていて, それは

$$3 + 5 = 2^3, \quad 3^3 + 5 = 2^5, \quad 3 + 5^3 = 2^7.$$

また, 対数の一次形式に関する Baker の理論 を用いれば, 方程式 $(*)$ の解 x, y, z の大きさの上界 (計算可能な正定数) を得ることが出来る. [5] によれば, (a, b, c のある仮定のもとで) $(*)$ のすべての解 (x, y, z) に対して, 次の評価を得ることが出来る:

$$\max\{x, y, z\} < 2^{288}\sqrt{abc}\log(abc).$$

Baker の理論によって得られる (上記の様な) 評価は, 方程式 $(*)$ の解を決定することにはあまり役に立たない. もし abc 予想を仮定すれば, 次の評価を得ることが出来る:

$$z = O\left(\frac{\log \prod_p p}{\log c}\right).$$

ここで p は abc のすべての素因数をわたる. 特に, $\prod_p p \leq abc$ より,

$$z = O\left(\frac{\log \max\{a, b, c\}}{\log c}\right)$$

を得る. これより, x, y の評価

$$x = O\left(\frac{\log \max\{a, b, c\}}{\log a}\right), \quad y = O\left(\frac{\log \max\{a, b, c\}}{\log b}\right)$$

も得られる. もし, 方程式 $(*)$ の項 a^x を正の整数 > 1 に置き換えるとき (x を固定するということと同じ), 方程式 $(*)$ は Pillai の方程式と呼ばれる (ここでは y, z が変数となる). Pillai の方程式に関する研究は数多くある. 特に, Bennett [1] は任意の Pillai の方程式は高々二つの解しか持たないことを証明している. 彼は, いくつかの有限個の三つ組み a, b, c を除いたとき, 解の個数は多くとも一つであると予想している.

一方で, 方程式 $(*)$ の解の決定に関する研究は, より活発である. もともとは, 方程式 $(*)$ は固定された三つ組み (a, b, c) について考察されていた. 初等整数論の様々な手法を用いて, a, b, c の値が小さい場合に, 方程式 $(*)$ の解が決定されてきた. 現在の多く研究は, 様々な三つ組み (a, b, c) の族に関するものである. 特に, 自然数 $p, q, r \geq 2$ に対して, $a^p + b^q = c^r$ を満たすものである. Jeśmanowicz [6] は, $p = q = r = 2$ の場合に, 方程式 $(*)$ はただ一つの解 $(x, y, z) = (2, 2, 2)$ を持つと予想している. これは, ピタゴラス数に関する未解決問題である. 寺井 [10] は, 一般の p, q, r に対して同様の問題を提起している.

この稿では, x, y が偶数となるような方程式 $(*)$ の解 x, y, z の上界を与える. また, その application として, a, b, c がフィボナッチ数で与えられる場合に方程式 $(*)$ を解く. $\{F_n\}_{n\geq 0}$ をフィボナッチ数列とする, すなわち $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$. フィボナッチ数は次の綺麗な公式を持つ:

$$F_n^2 + F_{n+1}^2 = F_{2n+1}.$$

ここで $n \geq 0$ ([7, p.79; Corollary 5.4] を参照). 上記の様な公式は, 他の線形回帰列ではみられないことに注意しておくことは価値がある. 2002 年の国際数学者会議の short communication において, 寺井 [11] は, $(a, b, c) = (F_n, F_{n+1}, F_{2n+1})$ の場合に, 各 $n \geq 3$ に対して方程式 $(*)$ はただ一つの解 $(x, y, z) = (2, 2, 1)$ を持つかどうか, という問題を提起した. この問題を以下の様に解くことが出来る.

Theorem F1. 各 $n \geq 3$ に対して, 方程式

$$F_n^x + F_{n+1}^y = F_{2n+1}^z$$

はただ一つの自然数解 $(x, y, z) = (2, 2, 1)$ を持つ.

2 Upper bounds for solutions

素数 p と整数 m $(\neq 0)$ に対して, $\mathrm{ord}_p(m)$ は m を p が割る最大の回数とする. また, m の p 部分を次で定める:

$$m_{(p)} := p^{\mathrm{ord}_p(m)}.$$

以下, b が偶数の場合を考える.

Theorem 1. (x,y,z) を $(*)$ の解とする. x,y,z をすべて偶数と仮定する. $x = 2X$, $y = 2Y$, $z = 2Z$ と書く (ここで X,Y,Z は自然数). このとき次の (i), (ii) が成り立つ.

(i)
$$X < \frac{2Y\log b - \log 4}{\log a}, \quad Z < \frac{2Y\log b - \log 2}{\log c}.$$

(ii) もし $Y > 1$ ならば,
$$Y \leq \frac{\log\min\{a+1,\, 2\sqrt{c-1}\,\}}{\log b_{(2)}}$$
が成り立つ.

Theorem 1 の証明

$\{a^X, b^Y, c^Z\}$ は原始ピタゴラス数なので,
$$a^X = k^2 - l^2, \quad b^Y = 2kl, \quad c^Z = k^2 + l^2,$$
ここで k,l は整数で, 次を満たす:
$$k > l > 0, \quad \gcd(k,l) = 1, \quad k \not\equiv l \pmod 2.$$
$(k+l)(k-l) = a^X$ かつ $\gcd(k+l, k-l) = 1$ なので,
$$k + l = u^X, \quad k - l = v^X,$$
と書ける. ここで u,v は整数で, 次を満たす:
$$u > v > 0, \quad \gcd(u,v) = 1, \quad uv = a.$$

不等式
$$a^X < k^2 = b^{2Y}/(4l^2), \quad c^Z < 2k^2 = b^{2Y}/(2l^2),$$
より, (i) はすぐにわかる.

(ii) ここから $Y > 1$ を仮定する. これから二通りの 2 進付値の計算を行い, Y の二通りの Y の上からの評価を得る. そのために次の補題を使う (証明は, [3, 4] にある):

Lemma. 自然数 $N \geq 2$ に対して, 方程式
$$X^{2N} + Y^4 = Z^2 \quad (X,Y,Z \in \mathbb{Z}\backslash\{0\},\ \gcd(X,Y) = 1)$$
は解を持たない.

Lemma. 自然数 $N \geq 2$ に対して, 方程式
$$X^{2N} + Y^2 = Z^4 \quad (X,Y,Z \in \mathbb{Z}\backslash\{0\},\ \gcd(X,Y) = 1,\ X \equiv 0 \pmod 2)$$
は解を持たない.

これより, X, Z は両方奇数であることが分かる. また, 二進付値の計算をするために次の補題を用いる ([9, p.11; P1.2] 参照).

Lemma. U と V は $U > V$ を満たす奇数, e を自然数とする. このとき

$$\mathrm{ord}_2(U^{2e} - V^{2e}) = \mathrm{ord}_2\bigl(U \pm V\bigr) + \mathrm{ord}_2(e) + 1$$

が, 適切な符号 ($U \pm V \equiv 0 \pmod 4$ となる符号) で成り立つ.

さて,

$$4kl = (k+l)^2 - (k-l)^2 = u^{2X} - v^{2X},$$

なので, 補題より,

$$\begin{aligned}\mathrm{ord}_2(b)\,Y &= \mathrm{ord}_2(b^Y)\\ &= \mathrm{ord}_2(2kl)\\ &= \mathrm{ord}_2\left(\frac{u^{2X} - v^{2X}}{2}\right)\\ &= \mathrm{ord}_2(u^{2X} - v^{2X}) - 1\\ &= \mathrm{ord}_2(u \pm v).\end{aligned}$$

さらに

$$u \pm v \leq u + v = a/v + v \leq a + 1,$$

なので,

$$Y = \frac{\mathrm{ord}_2\bigl(u + (-1)^{\frac{a+1}{2}} v\bigr)}{\mathrm{ord}_2(b)} \leq \frac{\log\bigl(a/p(a) + (-1)^{\frac{a+1}{2}} p(a)\bigr)}{\log b_{(2)}}$$

を得る.

一方で, $k^2 + l^2 = c^Z$ を書き換えて,

$$(k + l\sqrt{-1})(k - l\sqrt{-1}) = c^Z.$$

c が奇数であることから, 左辺の二因子は $\mathbb{Z}[\sqrt{-1}]$ で互いに素なので,

$$k + l\sqrt{-1} = (a_1 + b_1\sqrt{-1})^Z$$

となる整数 a_1, b_1 が存在し, $a_1^2 + b_1^2 = c$ が成り立つ. $a_1 \not\equiv b_1 \pmod 2$ に注意する. Z は奇数なので

$$\begin{aligned}k &= a_1\left(a_1^{Z-1} - \binom{Z}{Z-2} a_1^{Z-3} b_1^2 + \cdots \pm \binom{Z}{3} a_1^2 b_1^{Z-3} \pm Z b_1^{Z-1}\right),\\ l &= b_1\left(Z a_1^{Z-1} - \binom{Z}{Z-3} a_1^{Z-3} b_1^2 + \cdots \pm \binom{Z}{2} a_1^2 b_1^{Z-3} \pm b_1^{Z-1}\right).\end{aligned}$$

となる. 明らかに a_1 は k を割り切り, b_1 は l を割り切れない. 特に, a_1, b_1 は互いに素である. k/a_1 と l/b_1 が奇数であることをみるのは難しくない. よって

$$\mathrm{ord}_2(b)\,Y = \mathrm{ord}_2(b^Y) = \mathrm{ord}_2(2kl) = \mathrm{ord}_2(2a_1b_1).$$

$a_1 \not\equiv b_1 \pmod 2$ かつ $\max\{|a_1|, |b_1|\} \le \sqrt{c-1}$ なので,

$$Y = \frac{\mathrm{ord}_2(2a_1b_1)}{\mathrm{ord}_2(b)} \le \frac{\log(2\sqrt{c-1})}{\log b_{(2)}}$$

を得る (証明終).

同様の手法により, 次のことが証明される.

Theorem 2. (x, y, z) を $(*)$ の解とする. x, y を偶数, z を奇数と仮定する. $x = 2X$, $y = 2Y$ と書く (ここで X, Y は自然数). すると

$$Y \le \frac{\log(c-1)}{2\log b_{(2)}}$$

が成り立つ.

さらに, $c-1$ は平方数でない, または $c-1$ は b を割らない素因数を持つ, または

$$\frac{\log b}{\mathrm{ord}_2(b)} < \frac{\log(c-1)}{\mathrm{ord}_2(c-1)}$$

が成り立つ, または

$$Y \ne \frac{\mathrm{ord}_2(c-1)}{2\,\mathrm{ord}_2(b)}$$

が成り立つとする. このとき, 次の (i) または (ii) の一方だけが成り立つ:

$$\text{(i)} \quad X \le \frac{\log(c-4)}{\log a_{(p)}}, \quad z \le \min\left\{\frac{\log(c-1)}{\log c} M + \frac{1}{(c-1)^{M-m}\log c}, \sqrt{c-4}\right\},$$

$$\text{(ii)} \quad X \le \frac{2\log z}{\log a_{(p)}}, \quad \frac{z}{\log z} < \frac{2M}{\log c} + \frac{2}{(c-1)^{M-m}\log c\log(c-1)}, \quad z \ge \sqrt{c-1}.$$

ここで, p は $a_{(p)}$ が最少となる a の素因数である.

また, 不等式

$$M \le \frac{\sqrt{c}\log c}{\log(c-1)} - \frac{1}{(c-1)^{M-m}\log(c-1)}$$

が成立するときは, (i) が成り立つ.

3 Applications

$n \ge 3$ とする. F_n, F_{n+1}, F_{2n+1} はどの二つも互いに素な 1 より大の自然数であることに注意する. (x, y, z) を, 方程式

$$F_n^x + F_{n+1}^y = F_{2n+1}^z \tag{3.1}$$

の解とする．ここで x, y, z は自然数．初めに，合同式を用いて，x と y の偶奇性を確定させる．さらに，x, y, z の間の合同式を得る．

Lemma. 次の (i) と (ii) が成り立つ．

(i) x と y は偶数．

(ii) $X \equiv z \pmod{F_{n+1}}$ かつ $Y \equiv z \pmod{F_n}$，ここで $X = x/2$, $Y = y/2$.

Proof. 初めに $n = 3$ の場合を考える．このとき，方程式 (3.1) は

$$2^x + 3^y = 13^z. \tag{3.2}$$

(3.2) を法 3 でみると，$(-1)^x \equiv 1 \pmod 3$ となるので，x は偶数である．特に $x \geq 2$ である．すると 今度は (3.2) を法 4 でみると，$(-1)^y \equiv 1 \pmod 4$ となるので，y は偶数である．最後に (3.2) を法 5 でみると，$3^z \equiv \pm 2 \pmod 5$ となり，これより z は奇数となる．すると Theorem 2 より，$z = 1$ を得る．よって $x = y = 2$. ゆえに補題は $n = 3$ のとき成立する．同様にして $n = 4$ の時も証明される．したがって $n \geq 5$ を仮定してよい．

任意の $m \geq 4$ に対して，$F_{m+1} - F_m = F_{m-1} \geq F_3 = 2 > 1$ かつ $F_m > 1$. よって $F_m \not\equiv \pm 1 \pmod{F_{m+1}}$. 特に，次の合同式が成り立つ：

$$F_n \not\equiv \pm 1 \pmod{F_{n+1}}, \quad F_{n+1} \equiv F_{n-1} \not\equiv \pm 1 \pmod{F_n}.$$

$x = 2X + x_1$ と書く．ここで X は非負整数，$x_1 \in \{0, 1\}$ である．Cassini の等式から

$$F_n^2 = \delta + F_{n-1}F_{n+1} \equiv \delta - F_nF_{n+1} \pmod{F_{n+1}^2}.$$

ここで $\delta = (-1)^{n+1}$. よって

$$\begin{aligned} F_n^{2X} &= F_n^{2X}F_n^{x_1} \\ &\equiv (\delta - F_nF_{n+1})^X F_n^{x_1} \\ &\equiv (\delta^X - \delta^{X-1}F_nF_{n+1})F_n^{x_1} \pmod{F_{n+1}^2}, \end{aligned}$$

$$\begin{aligned} F_{2n+1}^z &= (F_n^2 + F_{n+1}^2)^z \\ &\equiv F_n^{2z} \\ &\equiv (\delta - F_nF_{n+1})^z \\ &\equiv \delta^z - \delta^{z-1}F_nF_{n+1}z \pmod{F_{n+1}^2}. \end{aligned}$$

したがって (3.1) から

$$(\delta^X - \delta^{X-1}F_nF_{n+1})F_n^{x_1} + F_{n+1}^y \equiv \delta^z - \delta^{z-1}F_nF_{n+1}z \pmod{F_{n+1}^2}.$$

これを法 F_{n+1} でみると，

$$\delta^X F_n^{x_1} \equiv \delta^z \pmod{F_{n+1}}.$$

もし $x_1 = 1$ ならば，$F_n \equiv \pm 1 \pmod{F_{n+1}}$ となるがこれは矛盾．よって $x_1 = 0$, すなわち，$x = 2X$. すると $\delta^X \equiv \delta^z \pmod{F_{n+1}}$. この合同式は，$\delta = \pm 1$ かつ $F_{n+1} \geq 3$ より，実際は等号であることがわかるので $\delta^X = \delta^z$. よって

$$-\delta^{X-1}F_nX + F_{n+1}^{y-1} \equiv -\delta^{X-1}F_nz \pmod{F_{n+1}}.$$

同様にして (3.1) を法 F_n^2 で考察することによって (合同式 $F_{n+1}^2 \equiv -\delta + F_n F_{n+1} \pmod{F_n^2}$), $F_{n+1} \not\equiv \pm 1 \pmod{F_n}$ を用いる), y は偶数であることと, 合同式

$$F_n^{x-1} + (-\delta)^{Y-1} F_{n+1} Y \equiv (-\delta)^{Y-1} F_{n+1} z \pmod{F_n},$$

を得る. ここで $Y = y/2$. x, y は 2 以上だから, 欲しい合同式 (ii) を得る. □

上の補題の (i) より, $x = 2X$, $y = 2Y$ と書ける. ここで X, Y は自然数である.

F_{2n+1} は奇数であると仮定してよい. 実際, F_{2n+1} は偶数である場合, F_n と F_{n+1} は奇数であり, よって $F_{2n+1}^z = F_n^{2X} + F_{n+1}^{2Y} \equiv 2 \pmod 4$ となる. これより $z = 1$ であり, $X = Y = 1$ を得る.

以下, F_{2n+1} は奇数である場合を考える. Theorem 2 を用いるために, 次の補題を示す.

Lemma. $F_{2n+1} - 1$ は, F_n, F_{n+1} それぞれを割らない素因数を持つ.

Proof. 初めに, F_n と L_n は F_{n+1} とは素であること, そして F_{n+1} と L_{n+1} は F_n と素であることに注意する. $F_{2n+1} = F_n^2 + F_{n+1}^2$ かつ $L_m = F_{m+1} + F_{m-1}$ $(m \geq 1)$, より, Cassini の等式から

$$F_{2n+1} - 1 = \begin{cases} F_n L_{n+1} & \text{if } n \text{ is even,} \\ L_n F_{n+1} & \text{if } n \text{ is odd.} \end{cases}$$

がわかる. これは補題を示している. □

定理の証明のためには,

$$\max\{X, Y\} \leq z$$

を示せばよいことは容易にわかる. 実際，もし上の不等式が成り立てば

$$(F_n^2 + F_{n+1}^2)^z = F_{2n+1}^z = F_n^{2X} + F_{n+1}^{2Y} \leq (F_n^2)^z + (F_{n+1}^2)^z$$

より, $z = 1$ となるので, $X = Y = 1$.
Theorem 1, 2 を用いると

$$\max(X, Y) \leq \frac{\log(F_{2n+1} - 1)}{\log 3}$$

を得る. すると $X - z$ と $Y - z$ の上からの評価は,

$$\begin{aligned} X - z &< X - \frac{2 \log F_n}{\log F_{2n+1}} X \\ &= \frac{\log(F_{2n+1}/F_n^2)}{\log F_{2n+1}} X \\ &= \frac{\log\bigl(1 + (F_{n+1}/F_n)^2\bigr)}{\log F_{2n+1}} X < \frac{\log\bigl(1 + (F_{n+1}/F_n)^2\bigr)}{\log 3} < 2, \end{aligned}$$

$$
\begin{aligned}
Y - z < Y - \frac{2\log F_{n+1}}{\log F_{2n+1}} Y \\
&= \frac{\log(F_{2n+1}/F_{n+1}^2)}{\log F_{2n+1}} Y \\
&= \frac{\log\bigl(1+(F_n/F_{n+1})^2\bigr)}{\log F_{2n+1}} Y < \frac{\log\bigl(1+(F_n/F_{n+1})^2\bigr)}{\log 3} < 1.
\end{aligned}
$$

したがって, (ii) より, $X - z \leq 0$ かつ $Y - z \leq 0$ となることがわかるので, $X = Y = z = 1$ を得る (証明終).

Remark. t の多項式列 $\{f_n(t)\}_{n\geq 0}$ を, $f_0(t) = 0$, $f_1(t) = 1$, $f_{n+2}(t) = t\,f_{n+1}(t) + f_n(t)$ で定義する. 明らかに $f_n(1) = F_n$. [7, Ch.37,38] によれば, 公式

$$f_n(t)^2 + f_{n+1}(t)^2 = f_{2n+1}(t)$$

が成立する $(n \geq 0)$. また, Cassini の等式と同様のものが成り立つ. Theorem F1 の証明と同様にして, 次のことを証明できる:

Theorem P1. 各 $n \geq 3$ と自然数 t に対して, 方程式

$$f_n(t)^x + f_{n+1}(t)^y = f_{2n+1}(t)^z$$

はただ一つの自然数解 $(x, y, z) = (2, 2, 1)$ を持つ.

これは Theorem F1 の一般化である.

Remark. フィボナッチ数には, 次の公式も知られている.

$$F_n^2 + F_{2n+2} = F_{n+2}^2.$$

よって, Theorem F1 で扱った問題と同様のものを提起できる. 実際, 次のことが証明できる.

Theorem F2. 各 $n \geq 3$ に対して, 方程式

$$F_n^x + F_{2n+2}^y = F_{n+2}^z$$

はただ一つの自然数解 $(x, y, z) = (2, 1, 2)$ を持つ.

t の多項式列 $\{B_n(t)\}_{n\geq 0}$ を $B_0(t) = 0$, $B_1(t) = 1$, $B_{n+2}(t) = t\,B_{n+1}(t) - B_n(t)$ で定義する. $B_n(3) = F_{2n}$ となることはすぐにわかる. [7, Ch.41] によれば, 公式

$$B_n(t)^2 + B_{2n+1}(t) = B_{n+1}(t)^2$$

が成り立つ $(n \geq 0)$. また, Cassini の等式と同様のものが成り立つ. Theorem F2 の証明と同様にして, 次のことを証明できる:

Theorem P2. 各 $n \geq 2$ と自然数 $t \geq 3$ に対して, 方程式

$$B_n(t)^x + B_{2n+1}(t)^y = B_{n+1}(t)^z$$

はただ一つの自然数解 $(x, y, z) = (2, 1, 2)$ を持つ.

これは Theorem F2 の部分的一般化である. Theorem F2, P2 の証明は省略する.

References

[1] M. A. Bennett, On some exponential equations of S. S. Pillai, *Canad. J. Math.* **53** (2001), 897–922.
[2] F. Beukers and H. P. Schlickewei, The equation $x + y = l$ in finitely generated groups, *Acta Arith.* **78** (1996), 189–199.
[3] Z. F. Cao and X. L. Dong, On the Terai-Jeśmanowicz conjecture, *Publ. Math. Debrecen* **22** (2002), 1–13.
[4] Z. F. Cao and X. L. Dong, An application of a lower bound for linear forms in two logarithms to the Terai-Jeśmanowicz conjecture, *Acta Arith.* **110** (2003), 153–164.
[5] N. Hirata-Kohno, S-unit equations and integer solutions to exponential Diophantine equations, *Analytic Number Theory and Surrounding Areas. RIMS Kokyuroku* **1511** (2006), 92–97.
[6] L. Jeśmanowicz, Several remarks on Pythagorean numbers, *Wiadom. Mat.* **1** (1955/56), 196–202 (in Polish).
[7] T. Koshy, *Fibonacci Numbers and Lucas Numbers with Applications* (Pure and Applied Mathematics, Wiley, 2001).
[8] K. Mahler, Zur Approximation algebraischer Zahlen I: Über den grössten Primteiler binärer Formen, *Math. Ann.* **107** (1933), 691–730.
[9] P. Ribenboim, *Catalan's Conjecture: Are* 8 *and* 9 *the only Consecutive Powers ?* (Boston, MA: Academic Press, 1994).
[10] N. Terai, Applications of a lower bound for linear forms in two logarithms to exponential Diophantine equations, *Acta Arith.* **90** (1999), 17–35.
[11] N. Terai, On an exponential Diophantine equation concerning Fibonacci numbers, *Abstracts of short communications and poster sessions: Beijing 2002 August 20 - 28*, International Congress of Mathematicians (Higher Education Press, 2002).

Department of Mathematics and Information Sciences, Tokyo Metropolitan University, 1-1, Minami-Ohsawa, Hachioji, Tokyo 192-0397, Japan
E-mail address: `miyazaki-takafumi@ed.tmu.ac.jp`